All unitary perfect polynomials over $\mathbb{F}_2$ with less than five distinct prime factors

Luis H. Gallardo - Olivier Rahavandrainy
Department of Mathematics, University of Brest,
6, Avenue Le Gorgeu, C.S. 93837, 29238 Brest Cedex 3, France.
e-mail : luisgall@univ-brest.fr - rahavand@univ-brest.fr

March 30, 2010

a) Running head: binary unitary perfect polynomials.

b) Keywords: Sum of divisors, unitary divisors, polynomials, finite fields, characteristic 2.

c) Mathematics Subject Classification (2000): 11T55, 11T06.

d) Corresponding author: Luis H. Gallardo.

Abstract We find all unitary perfect polynomials over the prime field $\mathbb{F}_2$ with less than five distinct prime factors.

1 Introduction

Let p be a prime number and let $\mathbb{F}_q$ be a finite field of characteristic p and order q. Let $A \in \mathbb{F}_q[x]$ be a monic polynomial. We say that a divisor d of A is unitary if d is monic and $\gcd(d, \frac{A}{d}) = 1$. Let $\omega(A)$ denote the number of distinct monic irreducible factors of A over $\mathbb{F}_q$ and let $\sigma(A)$ (resp. $\sigma^*(A)$) denote the sum of all monic divisors (resp. unitary divisors) of A (σ and σ^* are multiplicative functions).

The analogue notion over the positive integers is the notion of unitary perfect numbers. Only few results are known for them (see [15, 16, 19]), namely, all are even numbers, we know only five of them. Graham [16] characterized three of them, namely $6, 60, 87360$. Goto [15] proved an explicit exponential upper bound in $k = \omega(n)$ for n unitary perfect. Wall [19] improved a previous result of Subbarao, by proving that $\omega(n) \geq 9$ for any unitary perfect number n.

We call *even* a polynomial A with some zero in $\mathbb{F}_q$, and *odd* a polynomial that is not even. We assume that $A \notin \mathbb{F}_q$.

Since A and $\sigma(A)$ have the same degree it follows that A divides $\sigma(A)$ is equivalent to $\sigma(A) = A$. If $\sigma(A) = A$ (resp. $\sigma^*(A) = A$), then we say that A is a perfect (resp. unitary perfect) polynomial. We may consider the perfect polynomials as a polynomial analogue of the multiperfect numbers. E. F. Canaday, the first doctoral student of Leonard Carlitz, began in 1941 [5] the study of perfect polynomials by working on the prime field $\mathbb{F}_2$. Later, in the seventies, J. T. B. Beard Jr. et al. extended this work in several directions (see e.g. [2], [1], [4]) including the study of unitary perfect polynomials.

We became interested in this subject a few years ago and obtain some results ([6], [7], [8], [9], [10], [11], [12] and [13]) including for $q \in \{2, 4\}$ a complete classification of the perfect polynomials A for which $\omega(A)$ is small.

We began the study of unitary perfect polynomials by considering the splitting case when $q = p^2$ (see [14]). In this paper we study more general unitary perfect polynomials A improving on previous results of Beard et al. [3] and Beard [2]. In particular we prove that A must be even, contrary to perfect polynomials for which we do not know whether or not there exist odd

perfect polynomials. More precisely, we determine here all unitary perfect polynomials A, over $\mathbb{F}_2$, such that $\omega(A) \leq 4$. As usual $\mathbb{N}$ denotes the non-negative integers and $\mathbb{N}^*$ the positive integers.

Our main results are the following:

Let A be a nonconstant polynomial over $\mathbb{F}_2$ such that $\omega(A) \leq 4$, then A is unitary perfect if and only if either A or $A(x+1)$ is of the form B^{2^n} for some $n \in \mathbb{N}$ where:

– if $\omega(A) \leq 3$:

$B = x(x+1)$,
$B = x^3(x+1)^3(x^2+x+1)^2$,
$B(x) \in \{x^3(x+1)^2(x^2+x+1),\ x^5(x+1)^4(x^4+\cdots+x+1)\}$

– if $\omega(A) = 4$:

i) $B = x^6(x+1)^4(1+x+x^2)^3(1+x+x^4)$,
ii) $B = x^{13}(x+1)^8(1+x+x^2)^4(1+x+\cdots+x^{12})$,
iii) $B = x^{11}(x+1)^8(1+x+\cdots+x^4)^2(1+x+\cdots+x^{10})$,
iv) $B = x^9(x+1)^4(1+x+x^2)^2(1+x^3+x^6)$,
v) $B = x^{25}(x+1)^{16}(1+x+\cdots+x^4)^4(1+x^5+x^{10}+x^{15}+x^{20})$,
vi) $B = x^7(x+1)^4(1+x^2+x^3)(1+x+x^3)$,
vii) $B = x^3(x+1)^3(1+x+x^2)^3(1+x+x^4)$,
viii) $B = x^5(x+1)^6(1+x+x^2)^2(1+x+\cdots+x^4)$,
ix) $B = x^5(x+1)^5(1+x^3+x^4)(1+x+\cdots+x^4)$,
x) $B = x^{13}(x+1)^{12}(1+x+x^2)^8(1+x+\cdots+x^{12})$,
xi) $B = x^9(x+1)^6(1+x+x^2)^4(1+x^3+x^6)$,
xii) $B = x^7(x+1)^7(1+x+x^3)^2(1+x^2+x^3)^2$.

We may consider the family $\{x^{2^n}(x+1)^{2^n} : n \in \mathbb{N}\}$ as an analogue of the family $\{x^{2^n+1}(x+1)^{2^n+1}\}$ of trivial even perfect polynomials over $\mathbb{F}_2$.
Note that Beard [2] and Beard et al. [3] computed the above list with the exception of v), x), and xi) that are new.

Moreover, compared to the list of all perfect polynomials A over $\mathbb{F}_2$ with $\omega(A) < 5$ given in [11], we obtain an additional family of irreducible divisors

of unitary perfect polynomials:

$$\begin{array}{l} S_1(x) = 1 + x^3 + x^6,\ S_1(x+1), \\ S_2(x) = 1 + x^5 + x^{10} + x^{15} + x^{20},\ S_2(x+1) \\ S_3(x) = 1 + x + \cdots + x^{10},\ S_3(x+1), \\ S_4(x) = 1 + x + \cdots + x^{12},\ S_4(x+1). \end{array}$$

It is clear from the above results that the classification of all perfect or unitary perfect polynomials A with a moderately large number $\omega(A)$ of distinct prime factors may become very complicated. New tools need to be discovered to make more progress in this area.

2 Preliminary

We need the following results. Some of them are obvious, so we omit to give their proofs. Our first result give information on the sizes of the primary parts of unitary perfect polynomials.

Lemma 2.1. (see also [2, Theorem 1]) *If $A = P_1^{h_1} \cdots P_r^{h_r} Q_1^{k_1} \cdots Q_s^{k_s}$ is a nonconstant unitary perfect polynomial over $\mathbb{F}_q$ such that:*

$$\left\{ \begin{array}{l} P_1, \ldots, P_r, Q_1, \ldots, Q_s \text{are both irreducible} \\ h_1 \deg(P_1) = \cdots = h_r \deg(P_r) < k_1 \deg(Q_1) \leq \cdots \leq k_s \deg(Q_s). \end{array} \right.$$

Then:

$$r \equiv 0 \ (\mathrm{mod} p).$$

Proof. By definition, one has: $0 = \sigma^*(A) - A = \dfrac{A}{P_1^{h_1}} + \cdots + \dfrac{A}{P_r^{h_r}} + \cdots$

In particular, $r = 1 + \cdots + 1$, which is the leading coefficient of $\dfrac{A}{P_1^{h_1}} + \cdots + \dfrac{A}{P_r^{h_r}}$, equals 0 in $\mathbb{F}_p$. $\square$

Lemma 2.2. *If $A = A_1 A_2$ is unitary perfect over $\mathbb{F}_2$ and if* $\gcd(A_1, A_2) = 1$*. Then A_1 is unitary perfect if and only if A_2 is unitary perfect.*

Lemma 2.3. *If $A(x)$ is unitary perfect over $\mathbb{F}_2$, then the polynomials $A(x+1)$ and A^{2^n} are also unitary perfect over $\mathbb{F}_2$, for any $n \in \mathbb{N}$.*

We recall here some useful notation and results in Canaday's paper [5]:

- We define as the inverse of a polynomial $P(x)$ of degree m, the polynomial $P^*(x) = x^m P(\frac{1}{x})$.
- We say that P inverts into itself if $P = P^*$.
- A polynomial P is complete if $P = 1 + x + \cdots + x^h$, for some $h \in \mathbb{N}$.

Part iii) of the following lemma is essentially a result of Dickson (see [5, Lemma 2])

Lemma 2.4 (see [5, lemma 7], [11, Lemma 2.1])**.** i) *Any complete polynomial inverts into itself.* ii) *If $1 + x + \cdots + x^h = PQ$, where P, Q are irreducible, then either $(P = P^*, Q = Q^*)$ or $(P = Q^*, Q = P^*)$.*
iii) *If $P = P^*$, P irreducible and if $P = x^a(x+1)^b + 1$, then:*

$$P \in \{1 + x + x^2, 1 + x + \cdots + x^4\}.$$

Lemma 2.5. (see [5, Lemmata 4, 5, 6 and Theorem 8]) *Let $P, Q \in \mathbb{F}_2[x]$ such that P is irreducible and let $n, m \in \mathbb{N}$.*
i)*If $1 + P + \cdots + P^{2n} = Q^m$, then $m \in \{0, 1\}$.*
ii) *If $1 + P + \cdots + P^{2n} = Q^m A$, with $m > 1$ and $A \in \mathbb{F}_2[x]$ is nonconstant, then* $\deg(P) > \deg(Q)$.
iii) *If $1 + x + \cdots + x^{2n} = PQ$ and $P = 1 + (x+1) + \cdots + (x+1)^{2m}$, then $n = 4$, $P = 1 + x + x^2$ and $Q = P(x^3) = 1 + x^3 + x^6$.*
iv) *If any irreducible factor of $1 + x + \cdots + x^{2n}$ is of the form $x^a(x+1)^b + 1$, then $n \in \{1, 2, 3\}$.*
v) *If $1 + x + \cdots + x^h = 1 + (x+1) + \cdots + (x+1)^h$, then $h = 2^n - 2$, for some $n \in \mathbb{N}$.*

Lemma 2.6. *If $1 + x + x^2$ divides $1 + x + \cdots + x^h$, then $h \equiv 2 \mod 3$.*
If $1 + x + \cdots + x^4$ divides $1 + x + \cdots + x^h$, then $h \equiv 4 \mod 5$.

As a special case of [17, Theorem 2.47], we have

Lemma 2.7. *The polynomial $1 + x + \cdots + x^m$ is irreducible over $\mathbb{F}_2$ if and only if:*

$$m + 1 \text{ is a prime number and } 2 \text{ is a primitive root in } \mathbb{F}_{m+1}.$$

Consequently one gets

Lemma 2.8. i) *The polynomial* $Q(x) = 1 + x^5 + \cdots + (x^5)^l$ *is irreducible over* $\mathbb{F}_2$ *if and only if* $l = 4$.
ii) *The polynomial* $Q(x) = 1 + x + \cdots + x^{3.2^r}$ *is irreducible over* $\mathbb{F}_2$ *if and only if* $r = 2$.
iii) *The polynomial* $Q(x) = 1 + x + \cdots + x^{5.2^r}$ *is irreducible over* $\mathbb{F}_2$ *if and only if* $r = 1$.

Proof. We prove only necessity. Sufficiency is obtained by direct computations.
i): For $k \in \mathbb{N}^*$, let Φ_k be the k-th cyclotomic polynomial over $\mathbb{F}_2$. Recall that if k is a prime number, then $\Phi_k(x) = 1 + x + \cdots + x^{k-1}$.
If $Q(x)$ is irreducible, then $1 + x + \cdots + x^l$ is also irreducible.
Thus, by Lemma 2.7, $l + 1$ is a prime number and $Q(x) = \Phi_{l+1}(x^5)$.
It remains to observe that if $5 \neq l + 1$, then:

$$\Phi_{l+1}(x^5) = \Phi_{l+1}(x)\ \Phi_{5(l+1)}(x).$$

So that Q is not irreducible in that case. We conclude that $l = 4$.
ii): If $Q(x)$ is irreducible, then by Lemma 2.7, $p = 3\ .\ 2^r + 1$ is a prime number and 2 is a primitive root in $\mathbb{F}_p$. So, 2 is not a square in $\mathbb{F}_p$. By considering the Legendre Symbol $(\dfrac{2}{p}) = (-1)^{\frac{p^2-1}{8}}$, we see that we must have $r \in \{1, 2\}$.
The case $r = 1$ does not happen since $Q(x)$ is irreducible.
iii): As above, we obtain: $r \in \{1, 2\}$. The case $r = 2$ does not happen since $5.2^r + 1$ is prime. $\square$

We prove now the non-existence of odd unitary perfect polynomials:

Lemma 2.9. *Any nonconstant unitary perfect polynomial over* $\mathbb{F}_2$ *is divisible by* x *and by* $x + 1$. *In particular, there is no odd unitary perfect polynomial over* $\mathbb{F}_2$.

Proof. If P is an odd prime polynomial over $\mathbb{F}_2$, then $P(0) = P(1) = 1$, so that for any positive integer h, $1 + P(0)^h = 1 + P(1)^h = 0$. Thus, the monomials x and $x + 1$ divide $1 + P^h$. Now, let A be an unitary perfect polynomial. We have $\omega(A) \geq 2$. If both $x, x + 1$ divide A, then we are done. If there exists an odd polynomial $P \in \mathbb{F}_2[x]$ such that $P^h \mid A$ and $P^{h+1} \nmid A$, then $\sigma^*(P^h) = 1 + P^h$ divides $\sigma^*(A) = A$. So $x, x + 1$ divide A. $\square$

Remark 2.10. • *In the rest of the paper, we put $\overline{S}(x) = S(x+1)$ for $S \in \mathbb{F}_2[x]$.*

- *For Theorems 3.1 and 4.1, we shall prove only necessity, since sufficiency is always obtained by direct computations.*

3 Case $\omega(A) \leq 3$

We prove the following result:

Theorem 3.1. *Let $A \in \mathbb{F}_2[x]$ be a polynomial such that $\omega(A) \leq 3$, then A is unitary perfect over $\mathbb{F}_2$ if and only if either A or $\overline{A}$ is of the form B^{2^n} for some $n \in \mathbb{N}$, where:*

$$\begin{cases} i)\ B = x^2 + x, \\ ii)\ B \in \{x^3(x+1)^2(x^2+x+1),\ x^5(x+1)^4(x^4+\cdots+x+1)\}, \\ iii)\ B = x^3(x+1)^3(x^2+x+1)^2. \end{cases}$$

3.1 Case $\omega(A) = 2$

The following proposition gives the first part of Theorem 3.1.

Proposition 3.2. *Let $A \in \mathbb{F}_2[x]$ such that $\omega(A) = 2$, then A is unitary perfect over $\mathbb{F}_2$ if and only if A is of the form $(x^2+x)^{2^n}$, for some $n \in \mathbb{N}$.*

Proof. It remains to prove necessity since sufficiency is obvious.
The case where $A \in \{x^h P^k, (x+1)^h P^k\}$, with P odd, is impossible by Lemma 2.9. So A splits: $A = x^h (x+1)^k$. We must have: $1 + x^h = (x+1)^h,\ 1 + (x+1)^k = x^k$. Hence, $h = k = 2^n$, for some $n \in \mathbb{N}$. ☐

Consequently the unitary perfect polynomials A with $\omega(A) = 2$ are exactly the perfect polynomials with $\omega(A) = 2$.

3.2 Case $\omega(A) = 3$

In this case, A is of the form $x^{h_1}(x+1)^{k_1}P^l$, with P odd.

Lemma 3.3. *If $A = x^{h_1}(x+1)^{k_1}P^l$ is an unitary perfect polynomial over $\mathbb{F}_2$, then $l = 2^n$, for some nonnegative integer n.*

Proof. Put: $l = 2^n u$, where u is odd and $n \in \mathbb{N}$. Since the only prime divisors of $A = \sigma^*(A)$ are $x, x+1$ and P, and since P does not divide $1 + P^l$, the polynomial $1 + P^l = \sigma^*(P^l)$ must be of the form $x^a(x+1)^b$. Thus,

$$(1+P)(1+P+\cdots+P^{u-1}) = 1+P^u = x^c(x+1)^d.$$

Since $x, x+1$ divide $1+P$ and since $\gcd(1+P, 1+P+\cdots+P^{u-1}) = 1$, we conclude that $u-1=0$. $\square$

Put $h_1 = 2^h c,\ k_1 = 2^k d$ with c, d odd. Since A is unitary perfect, we have

$$\begin{cases} 1 + x^{h_1} = (x+1)^{2^h}(1+x+\cdots+x^{c-1})^{2^h}, \\ 1+(x+1)^{k_1} = x^{2^k}(1+(x+1)+\cdots+(x+1)^{d-1})^{2^k}, \\ 1+P^{2^n} = (1+P)^{2^n} = (x^{a_3}(x+1)^{b_3})^{2^n}. \end{cases} \tag{1}$$

Lemma 2.5-i) implies that:

$$1+x+\cdots+x^{c-1},\ 1+(x+1)+\cdots+(x+1)^{d-1} \in \{1, P\}.$$

Since h_1 and k_1 play symmetric roles and since P must appear in the right hand side of (1), we may reduce the study to the two cases:

$$\begin{aligned} &(\mathrm{I}) : 1+x+\cdots+x^{c-1} = P,\ d=1, \\ &(\mathrm{II}) : 1+x+\cdots+x^{c-1} = P = 1+(x+1)+\cdots+(x+1)^{d-1}. \end{aligned}$$

3.2.1 Case (I)

According to Lemma 2.4-iii), we have: $P \in \{1+x+x^2, 1+x+\cdots+x^4\}$ and $c \in \{3, 5\}$.
By considering exponents and degrees, System (1) implies

$$\begin{aligned} k = h+1, n = h \quad &\text{if } c = 3, \\ k = h+2, n = h \quad &\text{if } c = 5. \end{aligned}$$

We obtain part ii) of Theorem 3.1.

3.2.2 Case (II)

We have $c = d$ and $P = \overline{P}$. So, by Lemma 2.4, $P = 1+x+x^2$, and hence $c = d = 3$. System (1) implies: $k = h,\ n = h+1$, and we obtain part iii) of Theorem 3.1. This completes the proof of Theorem 3.1.

It turns out that we can also get Theorem 3.1. as a consequence of a nice result of Swan:

3.2.3 Another proof using Swan's Lemma

We would like to give, here, another proof of parts ii) and iii) of Theorem 3.1, by using Lemma 2.1 and the following result about reducibility of a binary polynomial in $\mathbb{F}_2[x]$:

Lemma 3.4 (see [18], p. 1103, line 3)**.** *Let $n, k \in \mathbb{N}$ be such that $8n > k$, then the polynomial $x^{8n} + x^k + 1$ is reducible over $\mathbb{F}_2$.*

From that, we obviously obtain the

Corollary 3.5. *Let r be a positive integer, then the polynomial*

$$P = x^{2^r} + x^{2^r - 1} + 1$$

is irreducible over $\mathbb{F}_2$ if and only if $r \in \{1, 2\}$.

We recall that A is of the form $x^{h_1}(x+1)^{k_1}P^l$, with P odd and $l = 2^n$ for some $n \in \mathbb{N}$. Put $p = \deg(P)$. By Lemma 2.1, we have either $(h_1 = k_1 \leq lp)$ or $(h_1 = lp \leq k_1)$ or $(k_1 = lp \leq h_1)$. The third case is similar to the second since h_1 and k_1 play symmetric roles.

<u>Case $h_1 = k_1 \leq lp$</u>

We obtain $A = x^{h_1}(x+1)^{h_1}P^{2^n}$, $h_1 \leq 2^n p$. Since A is unitary perfect, we have

$$\begin{aligned} &1 + x^{h_1} = (x+1)^{b_1} P^{c_1}, \\ &1 + (x+1)^{h_1} = x^{a_2} P^{c_2}, \\ &1 + P^{2^n} = (1+P)^{2^n} = (x^{a_3}(x+1)^{b_3})^{2^n}. \end{aligned}$$

Hence:

$$\begin{aligned} &P = x^{a_3}(x+1)^{b_3} + 1, \\ &(x+1)^{b_1} P^{c_1} = 1 + x^{h_1} = 1 + (x+1+1)^{h_1} = (x+1)^{a_2}(P(x+1))^{c_2}. \end{aligned}$$

It follows that:

$$a_2 = b_1, \; c_2 = c_1 \geq 1, \; P(x) = P(x+1).$$

Thus, $c_2 = c_1 = 2^{n-1}$ and $a_3 = b_3$. The irreducibility of P implies $a_3 = b_3 = 1$. So, $P = x^2 + x + 1$. Put $h_1 = 2^h c$, where c is odd. We have now:

$$(1+x)^{2^h}(1 + x + \cdots + x^{c-1})^{2^h} = 1 + x^{h_1} = (x+1)^{b_1}(x^2+x+1)^{2^{n-1}}.$$

Thus $c=3$ and $h=n-1$. We get $A=B^{2^{n-1}}$, where $B=x^3(x+1)^3(x^2+x+1)^2$. So we obtain part iii) of Theorem 3.1.

Case $h_1 = lp \leq k_1$

We obtain now: $A=x^{h_1}(x+1)^{k_1}P^{2^n}$, $h_1=2^n p \leq k_1$. Since A is unitary perfect, we have

$$\begin{array}{l} 1+x^{h_1}=(1+x^p)^{2^n}=((x+1)^{b_1}P^{c_1})^{2^n}, \\ 1+(x+1)^{k_1}=x^{a_2}P^{c_2}, \\ 1+P^{2^n}=(1+P)^{2^n}=(x^{a_3}(x+1)^{b_3})^{2^n}. \end{array}$$

Hence:

$$a_2+c_2p=k_1,\ b_1+c_1p=p,\ 2^n c_1+c_2=2^n.$$

It follows that $c_1 \in \{0,1\}$. If $c_1=0$, then $b_1=p$ and $1+x^p=(x+1)^p$, so $p=2^r$, for some $r \in \mathbb{N}^*$. Thus, $a_3+b_3=2^r$. Since $P=x^{a_3}(x+1)^{b_3}+1$ is irreducible, a_3 and b_3 must be both odd. Moreover, $c_2=2^n$ and

$$a_2+2^n\ 2^r=a_2+c_2p=k_1=2^n(b_1+b_3)=2^n(2^r+b_3).$$

Hence

$$a_2=2^n b_3,$$

and

$$(1+(x+1)^{2^r+b_3})^{2^n}=1+(x+1)^{k_1}=x^{a_2}P^{c_2}=(x^{b_3}P)^{2^n}.$$

It follows that:

$$1+(x+1)^{2^r+b_3}=x^{b_3}P=x^{b_3}(x^{a_3}(x+1)^{b_3}+1).$$

Thus,

$$b_3=1,\ a_3=2^r-1,\ k_1=2^n(2^r+1),\ P=x^{2^r-1}(x+1)+1,$$

and

$$A=(x^{2^r}(x+1)^{2^r+1}P)^{2^n}.$$

So by Corollary 3.5, we get $r \in \{1,2\}$ and $\overline{A}$ satisfies part ii) of Theorem 3.1. If $c_1=1$, then $c_2=b_1=0$. It follows that $1+x^p=P$, with $p \geq 2$. This contradicts the fact that P is irreducible.

4 Case $\omega(A) = 4$

We prove the following result:

Theorem 4.1. *Let $A \in \mathbb{F}_2[x]$ be a polynomial such that $\omega(A) = 4$, then A is unitary perfect over $\mathbb{F}_2$ if and only if either A or $\overline{A}$ is of the form B^{2^n} for some $n \in \mathbb{N}$, where:*

$$\begin{cases} i)\ B = x^6(x+1)^4(1+x+x^2)^3(1+x+x^4), \\ ii)\ B = x^{13}(x+1)^8(1+x+x^2)^4(1+x+\cdots+x^{12}), \\ iii)\ B = x^{11}(x+1)^8(1+x+\cdots+x^4)^2(1+x+\cdots+x^{10}), \\ iv)\ B = x^9(x+1)^4(1+x+x^2)^2(1+x^3+x^6), \\ v)\ B = x^{25}(x+1)^{16}(1+x+\cdots+x^4)^4(1+x^5+x^{10}+x^{15}+x^{20}), \\ vi)\ B = x^7(x+1)^4(1+x^2+x^3)(1+x+x^3), \\ vii)\ B = x^3(x+1)^3(1+x+x^2)^3(1+x+x^4), \\ viii)\ B = x^5(x+1)^6(1+x+x^2)^2(1+x+\cdots+x^4), \\ ix)\ B = x^5(x+1)^5(1+x^3+x^4)(1+x+\cdots+x^4), \\ x)\ B = x^{13}(x+1)^{12}(1+x+x^2)^8(1+x+\cdots+x^{12}), \\ xi)\ B = x^9(x+1)^6(1+x+x^2)^4(1+x^3+x^6), \\ xii)\ B = x^7(x+1)^7(1+x+x^3)^2(1+x^2+x^3)^2. \end{cases}$$

The following proposition gives more details about the form of an unitary perfect polynomial.

Proposition 4.2. *Every unitary perfect polynomial A over $\mathbb{F}_2$, with $\omega(A) = 4$, is of the form $x^{h_1}(x+1)^{k_1}P^{2^l u}Q^{2^m}$, where:*

i) P, Q, u are odd, $\deg(P) \leq \deg(Q)$,
ii) $h_1, k_1 \in \mathbb{N}^*$, $l, m \in \mathbb{N}$ and either $(u = 1)$ or $(u = 3,\ Q = 1 + P + P^2)$,
iii) $P \in \{1+x+x^2, 1+x+\cdots+x^4\}$ if P is complete,
iv) $\deg(Q) \geq 4$ if Q is complete.

Proof. First of all, x and $x+1$ divide A by Lemma 2.9. So

$$A = x^{h_1}(x+1)^{k_1}P^rQ^s,$$

for some $h_1, k_1, r, s \in \mathbb{N}^*$. Put $r = 2^l u,\ s = 2^m v$, where u, v are odd and $l, m \in \mathbb{N}$. Consider

$$\sigma^*(Q^s) = 1 + Q^s = (1+Q)^{2^m}(1+Q+\cdots+Q^{v-1})^{2^m}.$$

Since x and $x+1$ divide $1+Q$, they do not divide $1+Q+\cdots+Q^{v-1}$. Hence, $1+Q+\cdots+Q^{v-1} \in \{1, P\}$, by Lemma 2.5-i). If $v-1 \geq 2$, then $1+Q+\cdots+Q^{v-1} = P$. This is impossible because $\deg(P) \leq \deg(Q)$. Thus, $v-1=0$ and $s=2^m$. Now, by considering degrees, we see that the irreducible odd polynomial Q does not divide $1+P$. It follows that $(1+P)^{2^l}(1+P+\cdots+P^{u-1})^{2^l} = 1+P^r = \sigma^*(P^r)$ must be of the form $x^a(x+1)^bQ^c$. Thus, by Lemma 2.5-i):

$$1+P+\cdots+P^{u-1} \in \{1, Q\}.$$

We conclude that either $(u=1)$ or $(1+P+\cdots+P^{u-1}=Q)$.
If $u>1$, then put $u=2w+1$. We get

$$1+Q^{2^m} = (1+Q)^{2^m} = \Big(P(1+P+\cdots+P^{u-2})\Big)^{2^m} =$$

$$\Big(P(1+P)\big(1+P+\cdots+P^{w-1}\big)^2\Big)^{2^m}.$$

Since $x, x+1$ and P divide $1+Q$ and since $x, x+1$ divide $1+P$, none of the irreducible divisors of A does divide $1+P+\cdots+P^{w-1}$. Hence $w=1$, $u=3$ and $Q=1+P+P^2$. Since $\deg(P) \leq \deg(Q)$, the irreducible polynomial Q does not divide $1+P$. So P is always of the form $x^a(x+1)^b+1$. If P is complete, then by parts i) and iii) of Lemma 2.4, we have $P \in \{1+x+x^2, 1+x+\cdots+x^4\}$. Finally, if Q is complete, since $1+x+x^2$ is the only degree 2 odd irreducible polynomial over $\mathbb{F}_2$, we must have $\deg(Q) \geq 4$. $\square$

Put

$$p = \deg(P),\ q = \deg(Q),\ h_1 = 2^h c,\ k_1 = 2^k d, \text{ with } c, d \text{ odd}.$$

Since A is unitary perfect and since Q does not divide $1+P$, we have:

$$\begin{cases} 1+x^{h_1} = (1+x^c)^{2^h} = (1+x)^{2^h}(1+x+\cdots+x^{c-1})^{2^h} = (1+x)^{2^h}P^{2^h c_1}Q^{2^h d_1}, \\ 1+(x+1)^{k_1} = x^{2^k}(1+(1+x)+\cdots+(1+x)^{d-1})^{2^k} = x^{2^k}P^{2^k c_2}Q^{2^k d_2}, \\ 1+P^{2^l u} = (1+P)^{2^l}(1+P+\cdots+P^{u-1})^{2^l} = (x^{a_3}(1+x)^{b_3})^{2^l}Q^{2^l d_3}, \\ 1+Q^{2^m} = (1+Q)^{2^m} = (x^{a_4}(1+x)^{b_4}P^{c_4})^{2^m}. \end{cases} \tag{2}$$

By considering degrees and exponents of $x, x+1, P$ and Q, (2) implies:

$$\begin{cases} 2^h c = 2^h(1+pc_1+qd_1) = 2^k + 2^l a_3 + 2^m a_4, \\ 2^k d = 2^k(1+pc_2+qd_2) = 2^h + 2^l b_3 + 2^m b_4, \\ 2^l up = 2^l(a_3+b_3+qd_3) = (2^h c_1 + 2^k c_2 + 2^m c_4)p, \\ 2^m q = 2^m(a_4+b_4+pc_4) = (2^h d_1 + 2^k d_2 + 2^l d_3)q. \end{cases} \tag{3}$$

By Lemma 2.5, $c_1, d_1, c_2, d_2, d_3 \in \{0, 1\}$ so that:

$$1 + x + \cdots + x^{c-1},\ 1 + (1 + x) + \cdots + (1 + x)^{d-1} \in \{1, P, Q, PQ\}.$$

Since h_1 and k_1 play symmetric roles, and since $x, x+1, P$ and Q must divide $A = \sigma^*(A)$, it is sufficient to consider the following ten cases:

(I) : $c = d = 1$,
(II) : $1 + x + \cdots + x^{c-1} = P,\ d = 1$,
(III) : $1 + x + \cdots + x^{c-1} = Q,\ d = 1$,
(IV) : $1 + x + \cdots + x^{c-1} = PQ,\ d = 1$,
(V) : $1 + x + \cdots + x^{c-1} = P = 1 + (x + 1) + \cdots + (x + 1)^{d-1}$,
(VI) : $1 + x + \cdots + x^{c-1} = Q,\ 1 + (x + 1) + \cdots + (x + 1)^{d-1} = P$,
(VII) : $1 + x + \cdots + x^{c-1} = PQ,\ 1 + (x + 1) + \cdots + (x + 1)^{d-1} = P$,
(VIII) : $1 + x + \cdots + x^{c-1} = Q = 1 + (x + 1) + \cdots + (x + 1)^{d-1}$,
(IX) : $1 + x + \cdots + x^{c-1} = PQ,\ 1 + (x + 1) + \cdots + (x + 1)^{d-1} = Q$,
(X) : $1 + x + \cdots + x^{c-1} = PQ = 1 + (x + 1) + \cdots + (x + 1)^{d-1}$.

4.1 Case (I)

In this case, if $u = 1$, then since Q must appear in the right hand side of System (2), Q must divide $1 + P$, which is impossible. So, $u = 3$ and $1+Q = P(P+1)$. Thus, System (2) implies that $c_4 = 1$ and $3 \cdot 2^l = c_4 \cdot 2^m = 2^m$ so that 3 divides 2^m. It is impossible.

4.2 Case (II)

As above, $u = 3$ and $Q = 1 + P + P^2$. By Proposition 4.2, we get

$$P \in \{1 + x + x^2, 1 + x + \cdots + x^4\} \text{ and } c \in \{3, 5\}.$$

If $P = 1 + x + \cdots + x^4$, then:

$$Q = 1 + P + P^2 = 1 + x + x^3 + x^6 + x^8 = (1 + x + x^2)(1 + x^2 + x^4 + x^5 + x^6),$$

which is reducible.
So we must have: $P = 1 + x + x^2$. Thus, $c = 3$ and $Q = 1 + x + x^4$. System (3) implies that:

$$l = m,\ h = m + 1,\ k = m + 2.$$

We obtain part i) of Theorem 4.1.

4.3 Case (III)

P must divide $1+Q$ since it must appear in the right hand side of (2).
Put: $c-1=2^r s$, with s odd. We get

$$x^{a_4}(1+x)^{b_4+1}P^{c_4}=(1+x)(1+Q)=x(x+1)(1+x+\cdots+x^{c-2}).$$

Thus, $a_4=1$ and

$$(x+1)^{b_4+1}P^{c_4}=(1+x)(1+x+\cdots+x^{c-2})=1+x^{c-1}=(1+x)^{2^r}(1+x+\cdots+x^{s-1})^{2^r}.$$

We conclude that:

$$b_4=2^r-1,\ c_4=2^r,\ P=1+x+\cdots+x^{s-1}.$$

By Proposition 4.2, we get

$$P\in\{1+x+x^2,1+x+\cdots+x^4\}.$$

Thus, $c\in\{3\cdot 2^r+1,5\cdot 2^r+1\}$, and by Lemma 2.8, $c\in\{11,13\}$. It follows that we must have

$$\begin{array}{l} u=1,\ d_3=0,\\ P=1+x+x^2,\ Q=1+x+\cdots+x^{12}\ \text{ if } c=13,\\ P=1+x+\cdots+x^4,\ Q=1+x+\cdots+x^{10}\ \text{ if } c=11. \end{array}$$

System (3) implies

$$\begin{array}{l} m=h,\ l=h+2,\ k=h+3\ \text{ if } c=13,\\ m=h,\ l=h+1,\ k=h+3\ \text{ if } c=11. \end{array}$$

We obtain parts ii) and iii) of Theorem 4.1.

4.4 Case (IV)

We get $1+x+\cdots+x^{c-1}=PQ$, and by Lemma 2.4: $P\in\{P^*,Q^*\}$.

4.4.1 Case $P=P^*$

In this case, by Lemma 2.4-iii), we have: $P\in\{1+x+x^2,1+x+\cdots+x^4\}$.
• If $P=1+x+x^2$, then by Lemma 2.5-iii), the only possibility is

$$c=9,\ Q=1+x^3+x^6.$$

So, we must have

$$u = 1.$$

System (3) implies the following:

$$m = h, \ l = h + 1, \ k = h + 2.$$

We obtain then part iv) of Theorem 4.1.

- If $P = 1 + x + \cdots + x^4$, then $1 + x + \cdots + x^4$ divides $1 + x + \cdots + x^{c-1}$. So, by Lemma 2.6, c is divisible by 5. Put $c = 5w$. We get $Q = 1 + x^5 + x^{10} + \cdots + (x^5)^{w-1} \neq 1 + P + P^2$. Thus, by Lemma 2.8-i) and by Proposition 4.2, we have

$$c = 5w = 25, \ u = 1, \ P = 1 + x + \cdots + x^4, \ Q = 1 + x^5 + x^{10} + x^{15} + x^{20}.$$

System (3) implies

$$m = h, \ l = h + 2, \ k = h + 4.$$

So we obtain part v) of Theorem 4.1.

4.4.2 Case $P = Q^*$

We get $p = q$. So both P and Q are of the form $x^a(x+1)^b + 1$. We conclude by Lemma 2.5-iv) that:

$$c = 7, \ P, Q \in \{1 + x^2 + x^3, 1 + x + x^3\}.$$

It follows that $Q \neq 1 + P + P^2$ and $u = 1$. System (3) implies

$$l = m = h, \ k = h + 2.$$

We obtain then part vi) of Theorem 4.1.

4.5 Case (V)

In this case, by Lemma 2.4-iii), $P = 1 + x + x^2$ and $c = d = 3$. Moreover, u must be equal to 3. So, $Q = 1 + P + P^2 = 1 + x + x^4$. System (3) implies now:

$$l = m = k = h.$$

Consequently we obtain part vii) of Theorem 4.1.

4.6 Case (VI)

In this case, $\overline{P} \in \{1 + x + x^2, 1 + x + \cdots + x^4\}$ by Lemma 2.5-iv). So $Q \neq 1 + P + P^2$ and hence $u = 1$.

4.6.1 Case where P does not divide $1 + Q$

In this case, both P and Q are of the form $x^a(x+1)^b + 1$. By Lemma 2.5-iv) and Proposition 4.2-iii)-iv), we have two possibilities:

$$\begin{array}{l} \overline{P} = P = 1 + x + x^2, \ Q = 1 + x + \cdots + x^4, \\ \overline{P} = 1 + x + \cdots + x^4 = Q. \end{array}$$

Thus $(c, d) \in \{(5, 3), (5, 5)\}$. System (3) implies

$$\begin{array}{l} m = h, \ l = k = h + 1 \text{ if } c = 5, \ d = 3, \\ l = m = k = h \text{ if } c = d = 5. \end{array}$$

We obtain parts viii) and ix) of Theorem 4.1.

4.6.2 Case where P divides $1 + Q$

In this case, P must divide $\dfrac{1+Q}{x} = 1 + x + \cdots + x^{c-2}$. Moreover, according to System (2), we have

$$a_4 = 1, \ 1 + x + \cdots + x^{c-2} = (x + 1)^{b_4} P^{c_4}.$$

Thus, if we put $c - 1 = 2^r s$, with s odd, we obtain

$$(1 + x)^{2^r} (1 + x + \cdots + x^{s-1})^{2^r} = (1 + x^s)^{2^r} = 1 + x^{c-1} = (x + 1)^{b_4+1} P^{c_4}.$$

We conclude that:

$$b_4 = 2^r - 1,$$

and by Lemma 2.5-i):

$$P = 1 + x + \cdots + x^{s-1}, \ c_4 = 2^r.$$

Hence, by Lemmata 2.5-v) and 2.4-iii)the only possiblity that remains is

$$\overline{P} = 1 + x + x^2 = P, \ s = 3, \ c = 3 \cdot 2^r + 1.$$

It follows that $r = 2$ by Lemma 2.8. System (3) implies that:

$$m = h, \ k = h + 2, \ l = h + 3.$$

We obtain part x) of Theorem 4.1.

4.7 Case (VII)

In this case, P divides $1 + x + \cdots + x^{c-1}$. By Lemma 2.5-iii), we get

$$c = 9,\ P = 1 + x + x^2,\ d = 3,\ Q = 1 + x^3 + x^6.$$

Moreover, $u = 1$ since $Q \neq 1 + P + P^2$.
System (3) implies that:

$$m = h,\ k = h + 1,\ l = h + 2.$$

We obtain part xi) of Theorem 4.1.

4.8 Case (VIII)

In this case, by Lemma 2.5-v) and by Proposition 4.2-iv), $c = d = 2^w - 1 \geq 5$. Since P must appear in the right hand side of (2) , it must divide $1 + Q = x(1 + x + \cdots + x^{c-2})$. Hence P divides $1 + x + \cdots + x^{c-2}$. Thus,

$$a_4 = 1 \text{ and } (x+1)^{b_4} P^{c_4} = 1 + x + \cdots + x^{c-2} = (1+x)(1 + x + \cdots + x^{2^{w-1}-2})^2.$$

We deduce that:

$$b_4 = 1,\ c_4 = 2,\ P = 1 + x + \cdots + x^{2^{w-1}-2}.$$

By Proposition 4.2-iii), we must have

$$2^{w-1} - 2 \in \{2, 4\}.$$

So $w = 3$ and $Q = 1 + x + \cdots + x^7 = (1 + x)^7$ which is not irreducible.

4.9 Case (IX)

In this case, Q divides $1 + x + \cdots + x^{c-1}$. By Lemma 2.5-iii), we get

$$Q = 1 + x + x^2,\ P = 1 + x^3 + x^6.$$

This contradicts the fact: $\deg(P) \leq \deg(Q)$.

4.10 Case (X)

In this case, by Lemma 2.5-v), by Proposition 4.2-iv) and by Lemma 2.4-ii), we get

$$c = d = 2^w - 1 \geq 5, \text{ and either } (P = P^*, Q = Q^*) \text{ or } (P = Q^*).$$

4.10.1 Case where $P = P^*, \ Q = Q^*$

We have by Lemma 2.4-iii): $P \in \{1 + x + x^2, 1 + x + \cdots + x^4\}$.
• If $P = 1+x+x^2$, by Lemma 2.5-iii), $Q = 1+x^3+x^6$. Thus, $c = 9 = 2^w - 1$. This is impossible.
• If $P = 1 + x + \cdots + x^4$, then $\overline{P}$ divides $1 + x + \cdots + x^{d-1}$. So, by Lemma 2.5, $d - 1 = 8$. This is impossible.

4.10.2 Case where $P = Q^*$

We have $p = q$ and both P, Q are of the form $x^a(x + 1)^b + 1$. By Lemma 2.5-iv),

$$c = d = 7 \text{ and } P, Q \in \{1 + x + x^3, 1 + x^2 + x^3\}.$$

Moreover $u = 1$, by Proposition 4.2-ii). System (3) implies that:

$$l = m = h + 1, \ k = h.$$

We obtain finally part xii) of Theorem 4.1. This completes the proof of the Theorem.

5 Acknowledgments

We are grateful to the referee of a first version of this paper for careful reading and for suggestions that improved the presentation of the paper. We are including in the next section his report (but excluding the detailed technical suggestions to authors).

6 Report on preliminary version and conclusion

Referee report on the paper "All unitary perfect polynomials over F2 with less than five distinct prime factors" by Luis H. Gallardo and Olivier Rahavandrainy.

The authors are studying the problem of finding all the unitary perfect poly nomials over finite fields. The present paper contains the full classification of all the perfect unitary polynomials over F2 and serves as a continuation of a series of their publication devoted to the same topic. Previously

the problem was studied by E.F. Canaday, J.T.B. Beard Jr, A.T. Bulloc, M.S. Harbin, J.R. Oconnel Jr, K.I. West. The latest publication on study of the perfect unitary polynomials was published in 1991, and this makes papers of the mentioned authors hardly available. Moreover, publications [2]-[4] in the reference list is unavailable since the journal Rend. Acad. Lincei they published in has status "no longer indexed" in database of the AMS and the journal's webpage containing the mentioned volumes was not found. Happily the authors are citing the papers [2]-[4] only in the history of the question. The general idea of the proofs of the results in the paper is rather ele- mentary. But it requires a great scope of computations and applies more deep results on irreducibility of the polynomials. Some of these irreducibility results was proved by the authors in their previous papers. In general the paper makes good impression by numerous tricks used by the authors to simplify computations. The paper worth to be published in the Journal, it presents a new research which devoted to an interesting problem. The authors gives several interesting ideas, combination of which solves a problem. I found several misprints and places where arguments of proofs are not clear. I'd like to recommend the authors to correct misprints and clarify unclear arguments in proofs.

7 Conclusion

From the (seemingly favorable ?) report above it was deduced that the preliminary version of this paper was not suitable for publication in the IJNT.

References

[1] J. T. B. Beard Jr, *Perfect polynomials Revisited*, Publ. Math. Debrecen **38/1-2** (1991), 5–12.

[2] J. T. B. Beard Jr, *Unitary perfect polynomials over* $GF(q)$, Rend. Accad. Lincei **62** (1977), 417–422.

[3] J. T. B. Beard Jr, A. T. Bullock, M. S. Harbin, *Infinitely many perfect and unitary perfect polynomials*, Rend. Accad. Lincei **63** (1977), 294–303.

[4] J. T. B. Beard Jr, J. R. Oconnell Jr, K. I. West, *Perfect polynomials over $GF(q)$*, Rend. Accad. Lincei **62** (1977), 283–291.

[5] E. F. Canaday, *The sum of the divisors of a polynomial*, Duke Math. J. **8** (1941), 721–737.

[6] L. Gallardo, O. Rahavandrainy, *On perfect polynomials over $\mathbb{F}_4$*, Port. Math. (N.S.) **62(1)** (2005), 109–122.

[7] L. Gallardo, O. Rahavandrainy, *Perfect polynomials over $\mathbb{F}_4$ with less than five prime factors*, Port. Math. (N.S.) **64(1)** (2007), 21–38.

[8] L. H. Gallardo, O. Rahavandrainy, *Odd perfect polynomials over $\mathbb{F}_2$*, J. Théor. Nombres Bordeaux **19** (2007), 165–174.

[9] L. H. Gallardo, O. Rahavandrainy, *On splitting perfect polynomials over $\mathbb{F}_{p^p}$*, Preprint (2007).

[10] L. H. Gallardo, O. Rahavandrainy, *There is no odd perfect polynomial over $\mathbb{F}_2$ with four prime factors*, Port. Math. (N.S.) **66(2)** (2009), 131–145.

[11] L. H. Gallardo, O. Rahavandrainy, *Even perfect polynomials over $\mathbb{F}_2$ with four prime factors*, Intern. J. of Pure and Applied Math. **52(2)** (2009), 301–314.

[12] L. H. Gallardo, O. Rahavandrainy, *On splitting perfect polynomials over $\mathbb{F}_{p^2}$*, Port. Math. (N.S.) **66(3)** (2009), 261–273.

[13] L. H. Gallardo, O. Rahavandrainy, *All perfect polynomials with up to four prime factors over $\mathbb{F}_4$*, Math. Commun. **14(1)** (2009), 47–65.

[14] L. H. Gallardo, O. Rahavandrainy, *On unitary splitting perfect polynomials over $\mathbb{F}_{p^2}$*, Preprint (2009).

[15] Goto, Takeshi, *Upper bounds for unitary perfect numbers and unitary harmonic numbers*, Rocky Mountain J. Math. **37(5)** (2007), 1557–1576.

[16] Graham, S. W., *Unitary perfect numbers with squarefree odd part*, Fibonacci Quart. **26(4)** (1989), 312–317.

[17] R. Lidl, H. Niederreiter, *Finite Fields, Encyclopedia of Mathematics and its applications*, Cambridge University Press, 1983 (Reprinted 1987).

[18] R. G. Swan, *Factorization of polynomials over finite fields*, Pacific J. Math. **12** (1962), 1099–1106.

[19] Wall, Charles R., *New unitary perfect numbers have at least nine odd components*, Fibonacci Quart. **26(4)** (1988), 312–317.